UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,137	06/30/2003	Shawn E. Wiederin	COS02007	3010

25537 7590 08/11/2009

VERIZON
PATENT MANAGEMENT GROUP
1320 North Court House Road
9th Floor
ARLINGTON, VA 22201-2909

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
08/11/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/608,137
Filing Date: June 30, 2003
Appellant(s): WIEDERIN ET AL.

Meagan S. Walling
Reg. No. 60,112
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 26 January 2009 appealing from the Office action mailed 26 August 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0087882	SCHNEIER	7-2002
6,941,467	JUDGE	9-2005
6,519,703	JOYCE	2-2003
6,785,732	BATES	8-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 4, 5, 8-10, 12-14, 16, 19, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703.

Referring to claim 1, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of at least one interface configured to receive data transmitted via a network, a firewall configured to; receive data from the at least one interface, determine whether the data potentially contains malicious content. Interesting information collected from the firewall is sent to an anomaly engine ([0064]), which meets the limitation of identify first data in the received data that potentially contains malicious content, intrusion detection logic configured to: receive the first data. The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generate report information based on the first data, and forwarding logic configured to: receive the report information, forward the report information to a remote central management system when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the device. The anomaly engine receives only the information that cannot

be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed. However, Schneier does not explicitly disclose that the network traffic corresponding to this section of the report is forwarded for processing by a user application. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6), which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious because the purpose of filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known

technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 4, Schneier discloses that information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of a virtual private network gateway configured to establish a secure connection with the remote central management system.

Referring to claim 5, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of the firewall comprises anti-virus logic configured to examine a data stream for viral signatures using a signature-based technique.

Referring to claims 8, 9, Schneier discloses that the firewall receives filter updates from the SOC ([0037]), which meets the limitation of the firewall is configured to receive updated rule-based processing information from an external device via the network.

Referring to claim 10, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of receiving data transmitted via the network, identifying first data that may contain malicious content. Interesting information collected from the firewall is sent to an anomaly engine ([0064]). The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which

meets the limitations of generating report information based on the first data, forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the device. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed. However, Schneier does not explicitly disclose that the network traffic corresponding to this section of the report is forwarded for processing by a user application. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6), which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious because the purpose of

filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 12, Schneier discloses that the anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]). The information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of establishing a virtual private network connection to the external device, and wherein the forwarding the report information includes forwarding the report information over the virtual private network connection.

Referring to claim 13, Schneier discloses that the SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]). Schneier does not specify that SOC determination is applied to the network traffic that

corresponds to the report that was analyzed by the SOC. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6). If it is determined that the network traffic is malicious, then the network traffic is dropped (Col. 3, lines 48-54), which meets the limitation of receiving, from the external device, information indicating whether the first data is to be forwarded to the user device, and dropping the first data when the information indicates that the first data is not to be forwarded. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious or dropped when it is determined to be malicious because the purpose of filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique

of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 14, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of examining the received data for viruses using a signature-based technique.

Referring to claim 16, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of receive data transmitted via a network, determine whether the data may contain malicious content using a first set of rules. The firewall receives filter updates from the SOC ([0037]), which meets the limitation of receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data. Interesting information collected from the firewall is sent to an anomaly engine ([0064]), which meets the limitation of identify first data that may contain malicious content based on the determining. The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generate report information based on the first data, forward the report information to an external device when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the processor. The anomaly engine receives only the information that

cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed. However, Schneier does not explicitly disclose that the network traffic corresponding to this section of the report is forwarded for processing by a user application. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6), which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious because the purpose of filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known

technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 19, Schneier discloses that the anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]). The information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of establish a virtual private network tunnel with the external device and send the report information over the virtual private network tunnel.

Referring to claim 20, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of when identifying first data that may contain malicious content, the instructions cause the processor to identify a virus using a signature-based technique.

Claims 6, 15, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703, and further in view of Judge, U.S. Patent No. 6,941,467.

Referring to claims 6, 15, 21, Schneier does not specify that the firewall filters for spam. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to for the client-side firewall of Schneier to filter for spam because spam consumes resources that negatively impacts productivity as taught by Judge (Col. 4, lines 42-46).

Claims 7, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703, and further in view of Bates, U.S. Patent No. 6,785,732.

Referring to claims 7, 22, Schneier does not specify the type of data traffic that is received by the client-side. Bates discloses virus checking downloaded music files (Col. 10, lines 29-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made for virus-checking functionality in scan all types of data traffic, including downloaded music files, because computer viruses have emerged as a very real threat to data in today's computer systems, and checking files before they are downloaded would help to prevent virus infection as taught by Bates (Col. 1, lines 42-62).

(10) Response to Argument

Appellant argues, "SCHNEIER et al. and JOYCE do not disclose or suggest forwarding logic configured to forward report information to a remote central management system when the report information indicates that first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device." This argument is not persuasive because Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]). A resource coordinator forwards interesting information to a remote secure operations center (SOC) when further analysis is needed ([0064]). After further analysis, the SOC can inform the network response subsystem to not allow certain IP addresses to access the customer's network for a period of time ([0068]).

Appellant argues, "Because SCHNEIER et al. discloses a probe/sentry system that monitors and collects information concerning that status of a network and its components (paragraph 0035), there would be no reason for the sentry system of SCHNEIER et al. to make forwarding decisions." This argument is not persuasive because sentry system is not being relied upon to meet the claimed remote central management system. Instead the SOC of Schneier is relied upon to teach the claimed remote central management system. Since the SOC informs the network response subsystem of which IP address to not allow (i.e. block) access to the customer's network, the SOC effectively makes a forwarding decision on behalf of the sentry system (Figure 2).

Appellant argues, "This section of SCHNEIER et al. discloses blocking a certain IP address from accessing a customer's network. This section of SCHNEIER et al. has nothing to do with a remote management system that makes a forwarding decision on behalf of a device." This argument is not persuasive, because as mentioned above, the SOC makes a blocking decision (not to forward) on behalf of the probe/sentry system ([0068] & Figure 2).

Appellant arguments with respect to claims 10 and 12-14 (Section 2, brief pages 16-19), repeat the arguments made above. Examiner believes that the arguments have been fully addressed with the above responses.

Appellant arguments with respect to claims 16, 19, and 20 (Section 3, brief pages 19-22), repeat the arguments made above. Examiner believes that the arguments have been fully addressed with the above responses.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

Conferees:

/Jung Kim/
Primary Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432